(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003309558 A**

(43) Date of publication of application: **31.10.03**

(51) Int. Cl **H04L 9/32**
G06F 15/00
G09C 1/00
H04L 9/08
H04L 12/28
H04Q 7/38

(21) Application number: **2003026278**

(22) Date of filing: **03.02.03**

(30) Priority: **06.02.02 US 2002 066899**

(71) Applicant: **XEROX CORP**

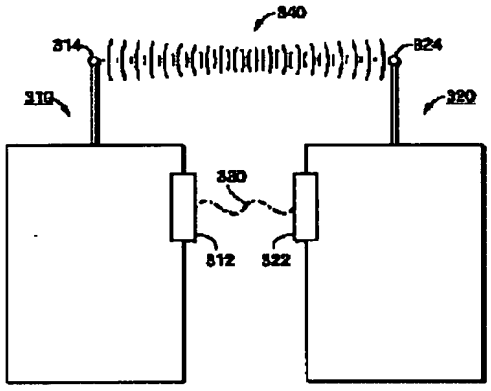
(72) Inventor: **BALFANZ DIRK**
LOPES CRISTINA V
SMETTERS DIANA K
STEWART PAUL JOSEPH
WONG HAO-CHI

(54) **METHOD FOR AUTHENTICATING COMMUNICATION ON NETWORK MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To guarantee the communication among a plurality of devices.

SOLUTION: This method for guaranteeing the communication between at least two devices on a network medium includes a step of transmitting previous authentication information from a first radio device 310 to a second radio device 320 on a position-limited channel, and a step of using the previous authentication information guaranteed by a second radio device 320 so as to authenticate the communication from the first radio device 310.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－309558
（P2003－309558A）
(43)公開日　平成15年10月31日(2003.10.31)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	15/00	３３０Ｃ　５Ｂ０８５
Ｇ０６Ｆ	15/00	３３０	Ｇ０９Ｃ	1/00	６４０Ｅ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｈ０４Ｌ	12/28	３００Ｚ　５Ｋ０３３
Ｈ０４Ｌ	9/08			9/00	６７５Ｂ　５Ｋ０６７
	12/28	３００	Ｈ０４Ｂ	7/26	１０９Ｒ

審査請求　未請求　請求項の数８　ＯＬ　（全 12 頁）　最終頁に続く

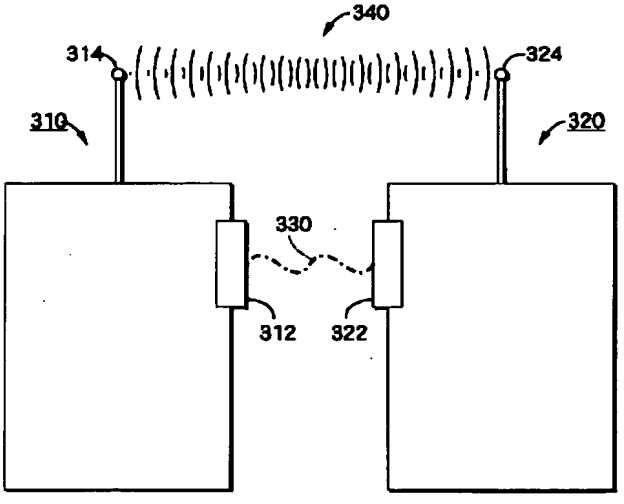
(21)出願番号　特願2003－26278(P2003－26278)
(22)出願日　平成15年２月３日(2003.2.3)
(31)優先権主張番号　１０／０６６，６９９
(32)優先日　平成14年２月６日(2002.2.6)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000798
ゼロックス・コーポレーション
アメリカ合衆国、コネチカット州、スタンフォード、ロング・リッジ・ロード　800
(72)発明者　ダーク　パルファンツ
アメリカ合衆国　カリフォルニア　メンロ　パーク　シャロン　パーク　ドライブ　600　アパートメント　ディー103
(74)代理人　100075258
弁理士　吉田　研二　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク媒体上で通信を認証するための方法

(57)【要約】
【課題】　複数のデバイス間の通信を保障する。
【解決手段】　ネットワーク媒体上における少なくとも２つのデバイス間での通信を保障する方法であって、位置限定チャネル上で第１の無線デバイス３１０から第２の無線デバイス３２０に事前認証情報を送信するステップと、第１の無線デバイス３１０からの通信を認証するため第２の無線デバイス３２０によって保障された事前認証情報を使用するステップとを含む方法。



1

【特許請求の範囲】
【請求項１】　ネットワーク媒体上における少なくとも２つのデバイス間での通信を保障する方法であって、
位置限定チャネル上で第１のデバイスから第２のデバイスに事前認証情報を送信するステップと、
前記第１のデバイスからの通信を認証するため前記第２のデバイスによって保障された前記事前認証情報を使用するステップと、
を含むことを特徴とする方法。
【請求項２】　請求項１に記載の方法であって、位置限定チャネル上で前記事前認証情報を送信するステップが、
少なくとも、第１のシークレットへのコミットメントおよび意味があるメッセージへのコミットメントを含むコミットメントを前記第１のデバイスから前記第２のデバイスに送るステップと、
少なくとも、第２のシークレットへのコミットメントおよび前記第２のデバイスから前記第１のデバイスへの意味がないメッセージへのコミットメントを含むコミットメントを送信することにより、前記第１のデバイスからのコミットメントに応答するステップと、
前記第１のデバイスによって前記第２のデバイスのコミットメントの受信を承認するステップと、
前記第２のデバイスによって前記第１のデバイスのコミットメントの受信を承認するステップと、
を含むことを特徴とする方法。
【請求項３】　ネットワーク媒体上におけるデバイスのグループ間での通信を保障する方法であって、
グループの少なくとも１つのデバイスをグループマネージャとして指定するステップと、
放送位置限定チャネルを使用して前記グループマネージャとグループの他のデバイスとの間の事前認証情報を交換するステップと、
前記交換された事前認証情報であって、ネットワーク媒体上で通信を認証するために前記グループマネージャと前記グループの他のデバイスとによって保障された事前認証情報を使用するステップと、
を含むことを特徴とする方法。
【請求項４】　請求項３に記載の方法であって、さらに、前記グループマネージャから前記グループ中の他のデバイスにグループキー情報を分配するためにネットワーク媒体を使用するステップを含むことを特徴とする方法。
【請求項５】　請求項３に記載の方法であって、さらに、
デバイスの前記グループ中に新しいデバイスを受信するステップと、
前記放送位置限定チャネルを使用して前記グループマネージャと前記新しいデバイスとの間で事前認証情報を交換するステップと、

2

前記交換された事前認証情報であって、ネットワーク媒体上で通信を認証するために前記グループマネージャと前記新しいデバイスとによって保障された事前認証情報を使用するステップと、
を含むことを特徴とする方法。
【請求項６】　請求項３に記載の方法であって、デバイスがデバイスの前記グループを離れる場合、さらに、
前記グループの他の残っているデバイスに対して前記グループマネージャの事前認証情報を無効にするステップと、
前記グループマネージャによって前記グループ中の残っているデバイスに新しい事前認証情報を分配するステップと、
前記グループマネージャと前記グループ中の残っているデバイスとによって分配された事前認証情報であって、前記グループマネージャと前記グループ中の残っているデバイスとの間での通信を認証する事前認証情報を使用するステップと、
を含むことを特徴とする方法。
【請求項７】　請求項６に記載の方法であって、さらに、前記グループマネージャから前記グループ中の残っているデバイスに新しいグループキー情報を分配するためにネットワーク媒体を使用するステップを含むことを特徴とする方法。
【請求項８】　ネットワーク媒体上におけるデバイスのグループ間での通信を認証する方法であって、
放送位置限定チャネル上で各デバイスとグループ中の他のデバイスとの間で事前認証情報を交換するステップと、
ネットワーク媒体上で選択されたデバイスとの通信を認証し通信しているデバイスによって保障された通信のために選択されたデバイスの事前認証情報を使用するステップと、
を含むことを特徴とする方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク媒体を使用して送信される少なくとも２つのデバイス間の通信を認証するためのシステムおよび方法に関する。
【０００２】
【従来の技術】ネットワーク通信によりユーザはネットワーク媒体上で文書などの情報を受信できるようになった。ネットワーク媒体は有線ネットワークおよび無線ネットワークを含む。ネットワーク媒体上で送信される情報は他者にとってアクセス可能である。しかしながら、ユーザは一般に受信されるそのような情報が他者にとって利用可能でないことを望む。
【０００３】
【発明が解決しようとする課題】本発明は、複数のデバイス間の通信を保障することを目的とする。

【０００４】

【課題を解決するための手段】本発明によれば、いくつかの無線デバイスを事前認証することを使用して、任意のピアツーピアアドホック（ｐｅｅｒ－ｔｏ－ｐｅｅｒ　ａｄ－ｈｏｃ）対話を確実に認証する。ここでは、暗号化チャネルをセットアップするために使用されるキー交換プロトコルへのブートストラップ（ｂｏｏｔｓｔｒａｐ）を含んでもよい。パブリックキーが事前認証チャネル上でコミットされる。パブリックキー暗号法を使用するキー交換プロトコルを主無線リンク中で使用して確実な通信を確立する。パブリックキーを使用して無線デバイスを事前認証するため、位置限定チャネル（ｌｏｃａｔｉｏｎ　ｌｉｍｉｔｅｄ　ｃｈａｎｎｅｌ）として使用可能な媒体のタイプは盗聴を心配する必要がなく、例えば可聴周波および／または赤外チャネルを含むことができる。パブリックキーを使用して無線デバイスを事前認証することにより、無線デバイスを認証することができる一連のパブリックキーベースキー交換プロトコルが使用できるようになる。

【０００５】

【発明の実施の形態】図１は無線システム３００の１つの例示的な実施形態を示す。２つだけの無線デバイス３１０および３２０が示されている。しかしながら、システム３００は３つ以上の無線デバイスを含むことができる。第１の無線デバイス３１０は位置限定チャネル受信機／送信機３１２および主無線リンク受信機／送信機３１４を含む。同様に、第２の無線デバイス３２０は位置限定チャネル受信機／送信機３２２および主無線リンク受信機／送信機３２４を含む。代替実施形態では、第１および第２の無線デバイスはそれぞれトランスポートコントロールプロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）ソケットや他の知られているかまたは後で開発された有線ネットワーク受信機／送信機などの主有線リンク受信機／送信機を有する。別の実施形態では、第１および第２の無線デバイスはどちらも主無線リンクおよび主有線リンクを有する。

【０００６】第１の無線デバイス３１０が第２の無線デバイス３２０との通信を開始した場合、第１の無線デバイス３１０は最初に事前認証情報を位置限定チャネル３３０を介して位置限定チャネル受信機／送信機３１２を通して第２の無線デバイス３２０に送る。第２の無線デバイス３２０は事前認証情報を第１の無線デバイス３１０から位置限定チャネル受信機／送信機３２２を通して受信する。

【０００７】相互認証が不要な場合、第１の無線デバイス３１０は第２の無線デバイス３２０に事前認証情報を送る必要はない。別の無線デバイスと事前認証情報を相互に交換しない無線デバイスは他の無線デバイスから受信した通信を認証することができない。したがって、その無線デバイスは盗聴者による攻撃から保護されない。

したがって、２つの無線デバイス間での機密情報の交換など、相互認証が必要な場合、第２の無線デバイス３２０は追加の事前認証情報を位置限定チャネル３３０を介して位置限定チャネル受信機／送信機３２２を通して無線デバイス３１０に送ることによって応答する。

【０００８】第１の無線デバイス３１０はそれの位置限定チャネル受信機／送信機３１２を通して事前認証情報を受信する。事前認証情報が第１の無線デバイス３１０と第２の無線デバイス３２０の間で交換されると、第１の無線デバイス３１０は主無線リンク受信機／送信機３１４を使用して主無線リンク３４０を介して第２の無線デバイス３２０と通信する。第２の無線デバイス３２０はそれの主無線リンク受信機／送信機３２４を使用して主無線リンク３４０を介して第１の無線デバイス３１０と通信する。事前認証情報が２つの無線デバイス３１０および３２０間で両方向に交換されているので、第１および第２の無線デバイス３１０および３２０の各々は、それぞれ他方の無線デバイス３２０または３１０から受信した受信事前認証情報を使用して、それぞれその他方の無線デバイス３２０または３１０の通信を認証する。

【０００９】図２は無線デバイス４００の１つの例示的な実施形態を示す。無線デバイス４００はパーソナルデジタルアシスタント（ＰＤＡ）、無線能力をもつラップトップコンピュータ、無線ハンドヘルドコンピュータ、Ｂｌａｃｋｂｅｒｒｙ（Ｒ）デバイス、無線能力をもつプリンタ、無線フォンなどとすることができる。無線デバイス４００は、プロセッサ４１０、メモリ４２０、入出力（Ｉ／Ｏ）インターフェース４３０、位置限定チャネル受信機／送信機４４２および主無線リンク受信機／送信機４４４を含む。

【００１０】メモリ４２０はオペレーティングシステム４２２、無線アプリケーション４２４、認証アプリケーション４２６および認証器４２８の各プログラムを記憶する。オペレーティングシステム４２２はプロセッサ４１０によって実行されると無線デバイス４００の入出力インターフェース４３０を含む様々な入出力コントローラをプログラムし、制御する。オペレーティングシステム４２２は無線アプリケーション４２４、認証アプリケーション４２６および認証器４２８を検索可能な様態で記憶する命令を提供する。

【００１１】無線アプリケーション４２４は無線デバイス４００が入出力インターフェース４３０の主無線リンクインターフェース４３４に接続された主無線リンク受信機／送信機４４４を通して無線ネットワークと通信できるようにする命令を提供する。無線アプリケーション４２４はＢｌｕｅｔｏｏｔｈ（Ｒ）、ＡＮＳＩ／ＩＥＥＥ８０２．１１などとすることができる。

【００１２】無線ネットワーク中で使用される無線受信機／送信機は主無線リンクインターフェース４３４および主無線リンク受信機／送信機４４４として使用するこ

とができる。代替実施形態では、無線デバイスはＴＣＰ／ＩＰインターフェースおよびソケットなどの主有線リンクインターフェースおよび主無線リンク受信機／送信機または主無線リンクインターフェースおよび送信機ならびに主有線インターフェースおよび受信機／送信機を有する。

【００１３】位置限定チャネル受信機／送信機４４２は主無線リンク受信機／送信機４４４とは別にすることができる。適切な位置限定チャネル受信機／送信機４４２は無線デバイスの事前認証情報を送受信するために少なくとも２つのプロパティを有する。第１のそのようなプロパティは例証的（ｄｅｍｏｎｓｔｒａｔｉｖｅ）プロパティである。適切な位置限定チャネル受信機／送信機４４２はそれの送信における物理的制限を有する。例えば、送信範囲および放送特性が制限されている、可聴周波範囲内および／または超音波範囲内の音声は無線デバイスのグループ用の位置限定チャネルとして使用されることがある。２つの無線デバイス間などポイントツーポイント通信では、赤外チャネルなど方向性をもつ位置限定チャネルが使用されることがある。例証的プロパティによればデバイスと位置限定チャネルを通してアクセス可能な限定された位置との間の物理的関係に基づいてターゲットデバイスまたはデバイスのグループを「名付ける」ために位置限定チャネル上で通信を行うことが可能になる。

【００１４】第２のプロパティは信頼性（ａｕｔｈｅｎｔｉｃｉｔｙ）である。このプロパティによれば、盗聴が存在する場合でも、位置限定チャネル上で交換される事前認証情報により交換している無線デバイスが主無線リンク上で互いを確実に認証することができる。関係者が位置限定チャネルを使用してそれらのパブリックキーを事前認証情報として交換する場合、盗聴者は関係者のプライベートキーを知らないので位置限定チャネル上での盗聴者による攻撃は重要ではない。関係者はキー交換プロトコルの一部としてそれらの対応するプライベートキーの保有を証明することによって主無線リンク上で互いを認証することになる。したがって、盗聴者はいずれの関係者をも装うことができない。

【００１５】位置限定チャネル受信機／送信機の別のプロパティは、攻撃が少なくとも１つの合法参加者（人間またはデバイス）によって検出されることなしに位置限定チャネルを攻撃することが困難なことである。これらは赤外、可聴周波および／または超音波の音声、および／または本体上での近接場信号を使用する受信機／送信機を含む。

【００１６】攻撃を検出する場合、位置限定チャネル上で送信しているデバイスが特定される必要はないことがある。代わりに、例えば、攻撃を検出することは単に人の計数する能力に依存することがある。したがって、２つの無線デバイスが通信しようと試み、例えばターゲットデバイス上の光が明滅することによって、またはラップトップコンピュータを使用している人間が通信が成功したことを示すことによって、通信が成功したことが示された場合、合法関係者の数が知れる。例えば、第３の関係者が通信に参加していることをラップトップが示すことによって、余分な違法の関係者が検出された場合、通信は単に合法関係者によって中止されることがある。

【００１７】事前認証情報は受信した認証器４２８を認証するために使用される。認証器４２８はキー、シークレットなどとすることができる。キーは長命キーかまたは短命キーとすることができる。選択は通常キーが使用されているアプリケーションに基づく。いずれの場合にも、キーは信用されている権威による証明を必要としない。しかしながら、選択されるキー交換プロトコルが証明書の交換を必要とする場合、証明書は無線デバイス４００によって自己署名される。

【００１８】通常、位置限定チャネル上で交換される情報の量は主無線リンク上で送られる情報の量の小部分である。事前認証情報のサイズを縮小する１つの方法は、例えばＳｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ－１（ＳＨＡ－１）などの暗号法上安全なハッシュ関数を使用することである。この方法を使用すると、関係者は実際にそれらの完全なパブリックキーを事前認証情報として交換する必要がない。代わりに、関係者は、例えばキーのダイジェストを交換することによってキーのコミットメントを送る。関係者は選択された位置限定チャネル上でそれらのパブリックキーへのコミットメントを交換する。そうすることで、各関係者は、その関係者が通信している人を特定することができる。

【００１９】無線デバイス４００は主無線リンク受信機／送信機４４４を使用して別の無線デバイスと通信する。無線デバイス４００は、市販されているＳｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ／Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＳＳＬ／ＴＬＳ）、Ｓｅｃｕｒｅ Ｋｅｙ Ｅｘｃｈａｎｇｅ Ｍｅｃｈａｎｉｓｍ（ＳＫＥＭＥ）、Ｉｎｔｅｒｎｅｔ Ｋｅｙ Ｅｘｃｈａｎｇｅ（ＩＫＥ）などの様々な確立されたパブリックキーベースキー交換プロトコルを含む認証アプリケーション４２６を使用して、事前認証情報交換中にコミットされたパブリックキーに対応するプライベートキーの保有を証明する。その場合、パブリックキーのダイジェストが事前認証情報交換中に送られた場合、無線デバイス４００は主無線リンク上で完全なパブリックキーを交換する。キー交換はプロトコル実行にプレフィクスされるか、またはＳｏｃｋｅｔ Ｌａｙｅｒ／Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＳＳＬ／ＴＬＳ）の場合のように、キー交換プロトコルの標準部分として当然行われる。キーはそれらが位置限定チャネル上でコミットされたものであったという事実によって認証される。他の無線デバイスのパブリックキーを認証

した無線デバイス４００は主無線リンク上で交換プロトコルを続行する。

【００２０】図３はネットワーク媒体上で通信を認証する１つの方法を概説するフローチャートである。ステップＳ１００から始めて、オペレーションはステップＳ１１０に進み、そこで第１の無線デバイスは第２の無線デバイスに位置限定チャネルを使用してパブリックキーＰＫ$_1$へのコミットメントを送る。これは位置限定チャネル上での事前認証情報の交換の少なくとも一部である。コミットメントはパブリックキー自体、証明書、またはパブリックキーのダイジェストとすることができる。ステップＳ１２０で、第１の無線デバイスからパブリックキーＰＫ$_1$へのコミットメントを受信したことに応答して、第２の無線デバイスは第１の無線デバイスによって受信される位置限定チャネル上でパブリックキーＰＫ$_2$へのコミットメントを送る。この段階で、第１の無線デバイスは主無線リンク上での通信に備えるために第２の無線デバイスのアドレスを受信することもできる。

【００２１】ステップＳ１３０で、第１の無線デバイスは主無線リンクを使用して第２の無線デバイスにパブリックキーＰＫ$_1$を送る。ステップＳ１４０で、第２の無線デバイスはそれのパブリックキーＰＫ$_2$を第１の無線デバイスに送り、キーの交換が行われる。ステップＳ１５０で、第１の無線デバイスは第２の無線デバイスから受信したパブリックキーＰＫ$_2$を認証し、パブリックキーＰＫ$_2$を事前認証情報段階で受信したコミットメントと比較する。一実施形態では、受信したパブリックキーＰＫ$_2$の認証は、パブリックキーに対応するプライベートキーの所有権を証明する図２に示されるものなどのキー交換プロトコルを使用して実施される。第１の無線デバイスがそれのパブリックキーＰＫ$_1$を主無線リンク上で送るときに第２の無線デバイスがシークレットＳ$_2$を使用している場合、第２の無線デバイスはパブリックキーＰＫ$_1$をコミットメントに対して検証し、それを使用してそれのシークレットＳ$_2$を暗号化し、結果ＥＰＫ$_1$（Ｓ$_2$）を第１の無線デバイスに戻す。認証はシークレットＳ$_2$を生成する第２の無線デバイスの能力および結果ＥＰＫ$_1$（Ｓ$_2$）を復号する第１の無線デバイスの能力によって実施される。

【００２２】ステップＳ１６０で、前に第２の無線デバイスから受信したパブリックキーＰＫ$_2$のコミットメントが受信したパブリックキーＰＫ$_2$に一致するかどうかの決定がなされる。そうである場合、オペレーションはステップＳ１７０に進む。それ以外の場合、オペレーションはステップＳ１８０に飛ぶ。Ｓ１７０において第１の無線デバイスは、通信を暗号化するためにキー交換プロトコル中に同意された対称キーを使用して主無線リンク上で第２の無線デバイスとの通信を再開する。次いでオペレーションはＳ１９０に飛ぶ。反対に、ステップＳ１８０で、第１の無線デバイスが第２の無線デバイスのパブリックキーＰＫ$_2$を認証することができない場合、第１の無線デバイスは第２の無線デバイスとの通信を終了する。次いでオペレーションはステップＳ１９０に進み、そこで方法は終わる。

【００２３】様々な例示的な実施形態では、第１の無線デバイスは乱数などの任意のシークレットＳ$_1$を含むことを理解されたい。この場合、第１の無線デバイスは任意のシークレットＳ$_1$へのコミットメントを送っているので、Ｓ$_1$はシークレットのままであるべきなのでコミットメントは暗号法ダイジェストｈ（Ｓ$_1$）の形態で送られる。様々な他の例示的な実施形態では、第１の無線デバイスは、主無線リンクでの通信に備えるためにＩＰアドレスおよびポート番号、Ｂｌｕｅｔｏｏｔｈデバイスアドレス、ユーザフレンドリ名または他の適切な情報など、それのアドレスを送信することもできる。

【００２４】図４～図６は、対話通信に備える改善されたＧｕｙ　Ｆａｗｋｅｓプロトコルを実施する方法の１つの例示的な実施形態を概説するフローチャートである。この方法は、パブリックキーオペレーションが実行不可能であるような無線デバイスの計算リソースが制限されており、位置限定チャネルがシークレットデータの信用されている交換を提供しない場合に使用することができる。

【００２５】図４～図６に示すように、オペレーションはステップＳ２００で始まり、ステップＳ２０５に進み、そこでカウンタＮは１にセットされる。ステップＳ２１０で、第１の無線デバイスは、第２の無線デバイスに位置限定チャネル上でそれのＮ番目のメッセージのダイジェストとともにそれのＮ番目のメッセージを認証するために使用されることになるそれのＮ番目のシークレット（認証器）のダイジェストを含むＮ番目の通信を送る。ステップＳ２１５で、第２の無線デバイスは、第１の無線デバイスに位置限定チャネル上でそれのＮ番目のメッセージのダイジェストとともにそれのＮ番目のメッセージを認証するために使用されることになるそれのＮ番目のシークレットのダイジェストを含むＮ番目の通信を送る。

【００２６】ステップＳ２２０で、第１の無線デバイスは第２の無線デバイスに第２の無線デバイスのＮ番目の通信のダイジェストおよび第１の無線デバイスのＮ番目のシークレットを送る。ステップ２２５で、第２の無線デバイスは第１の無線デバイスに第１の無線デバイスのＮ番目の通信のダイジェストおよび第２の無線デバイスのＮ番目のシークレットを送る。ステップＳ２３０で、第１および第２の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第１の無線デバイスかまたは第２の無線デバイスが通信を終了すると決定した場合、オペレーションはステップＳ３２０に進む。その他の場合、通信は継続し、オペレーションはステップＳ２３５に進む。

【００２７】ステップＳ２３５で、第１の無線デバイスは主無線リンク上で通信を継続する。通信の開始者として、第１の無線デバイスは、第２の無線デバイスに、意味があるＮ番目のメッセージと、（Ｎ＋１）番目のメッセージのダイジェストを含む（Ｎ＋１）番目の通信とともにそれの（Ｎ＋１）番目のメッセージを認証するために使用されることになるそれの（Ｎ＋１）番目のシークレットのダイジェストとを送る。ステップＳ２４０で、第２の無線デバイスは、第１の無線デバイスに、意味がないＮ番目のメッセージと、（Ｎ＋１）番目のメッセージのダイジェストを含む（Ｎ＋１）番目の通信とともにそれの（Ｎ＋１）番目のメッセージを認証するために使用されることになるそれの（Ｎ＋１）番目のシークレットのダイジェストとを送る。第２の無線デバイスのＮ番目のメッセージは、第２の無線デバイスがステップＳ２１０で送信された第１の無線デバイスのＮ番目のメッセージを知らないときにステップＳ２１５でコミットされたものなので意味がない。この時点で、無線デバイスのいずれかが通信を終了することができる。したがって、ステップＳ２４５で、第１および第２の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第１の無線デバイスかまたは第２の無線デバイスが通信を終了すると決定した場合、オペレーションはステップＳ３２０に進む。その他の場合、通信は継続し、オペレーションはステップＳ２５０に進む。

【００２８】ステップＳ２５０で、第１の無線デバイスは第２の無線デバイスに第２の無線デバイスの（Ｎ＋１）番目の通信のダイジェストおよび第１の無線デバイスの（Ｎ＋１）番目のシークレットを送る。ステップＳ２５５で、第２の無線デバイスは第１の無線デバイスに第１の無線デバイスの（Ｎ＋１）番目の通信のダイジェストおよび第２の無線デバイスの（Ｎ＋１）番目のシークレットを送る。

【００２９】ステップＳ２６０で、第１の無線デバイスは、第２の無線デバイスに、意味がない（Ｎ＋１）番目のメッセージと、（Ｎ＋２）番目のメッセージのダイジェストを含む（Ｎ＋２）番目の通信とともにそれの（Ｎ＋２）番目のメッセージを認証するために使用されることになるそれの（Ｎ＋２）番目のシークレットのダイジェストとを送る。第１の無線デバイスの（Ｎ＋１）番目のメッセージは、意味があるメッセージを送る順番が第２の無線デバイスなので意味がない。ステップＳ２６５で、第２の無線デバイスは、第１の無線デバイスに、意味がある（Ｎ＋１）番目のメッセージと、（Ｎ＋２）番目のメッセージのダイジェストを含む（Ｎ＋２）番目の通信とともにそれの（Ｎ＋２）番目のメッセージを認証するために使用されることになるそれの（Ｎ＋２）番目のシークレットのダイジェストとを送る。第２の無線デバイスは、第２の無線デバイスが意味がある第１の無線デバイスのＮ番目のメッセージを知った後でステップＳ２４０でコミットメントがなされたために意味があるメッセージを送る。ステップＳ２７０で、第１および第２の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第１の無線デバイスかまたは第２の無線デバイスが通信を終了すると決定した場合、オペレーションはステップＳ３２０に進む。その他の場合、通信は継続し、オペレーションはステップＳ２７５に進む。

【００３０】ステップＳ２７５で、第１の無線デバイスは第２の無線デバイスに第２の無線デバイスの（Ｎ＋２）番目の通信のダイジェストおよび第１の無線デバイスの（Ｎ＋２）番目のシークレットを送る。次に、ステップＳ２８０で、第２の無線デバイスは第１の無線デバイスに第１の無線デバイスの（Ｎ＋２）番目の通信のダイジェストおよび第２の無線デバイスの（Ｎ＋２）番目のシークレットを送る。ステップＳ２８５で、第１の無線デバイスは、第２の無線デバイスに、意味がない（Ｎ＋２）番目のメッセージと、（Ｎ＋３）番目のメッセージのダイジェストを含む（Ｎ＋３）番目の通信とともにそれの（Ｎ＋３）番目のメッセージを認証するために使用されることになるそれの（Ｎ＋３）番目のシークレットのダイジェストとを送る。（Ｎ＋２）番目のメッセージは、第１の無線デバイスが意味がある第２の無線デバイスの（Ｎ＋１）番目のメッセージを受信していないときに第１の無線デバイスがステップＳ２６０でコミットされたので意味がない。しかしながら、第１の無線デバイスは、第１の無線デバイスがステップＳ２６５で第２の無線デバイスからの意味がある（Ｎ＋１）番目のメッセージを有していたので意味がある（Ｎ＋３）番目のメッセージにコミットすることができる。

【００３１】ステップＳ２９０で、第２の無線デバイスは、第１の無線デバイスに、意味がない（Ｎ＋２）番目のメッセージと、（Ｎ＋３）番目のメッセージのダイジェストを含む（Ｎ＋３）番目の通信とともにそれの（Ｎ＋３）番目のメッセージを認証するために使用されることになるそれの（Ｎ＋３）番目のシークレットのダイジェストとを送る。第２の無線デバイスの（Ｎ＋２）番目のメッセージは、「話す」次の順番が第１の無線デバイスに属するので意味がない。この場合も、この時点で、無線デバイスのいずれかが通信を終了することができる。したがって、ステップＳ２９５で、第１および第２の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第１の無線デバイスかまたは第２の無線デバイスが通信を終了すると決定した場合、オペレーションはステップＳ３２０に飛ぶ。その他の場合、通信は継続し、オペレーションはステップＳ３００に進む。

【００３２】ステップＳ３００で、第１の無線デバイスは第２の無線デバイスに第２の無線デバイスの（Ｎ＋３）番目の通信のダイジェストおよび第１の無線デバイ

スの（Ｎ＋３）番目のシークレットを送る。ステップＳ３０５で、第２の無線デバイスは第１の無線デバイスに第１の無線デバイスの（Ｎ＋３）番目の通信のダイジェストおよび第２の無線デバイスの（Ｎ＋３）番目のシークレットを送る。ステップＳ３１０で、コントローラＮは４に増分される。次いでオペレーションはステップＳ２３５に戻る。反対に、ステップＳ３２０で、方法のオペレーションは終わる。

【００３３】相互認証が不要であるアプリケーションがあることを理解されたい。例えば、サービスを要求する誰かにサービスを提供するように設計されたデバイスは、それが通信しているデバイスを認証する必要はなく、したがって事前認証情報を送るべき唯一のデバイスとすることができる。そのようなデバイスは、例えば、無線空間中でそれの能動的プロキシを一意的にかつ確実に特定するのに十分な事前認証情報を送る赤外（ＩＲ）情報ビーコンまたは無線周波数特定（ＲＦＩｄ）タグなどの受動的ビーコンを有することができる。そのような手法は、物理的目標に「デジタル存在」を提供するためにそのようなビーコンを使用するシステムにセキュリティおよび認証の尺度を追加するために使用することができる。

【００３４】図２に関して説明した位置限定チャネルの一部は放送能力を有する。そのような放送能力を使用すると、認証されたグループ通信に備えるプロトコルを構成することができる。アプリケーションにはネットワーク化されたゲームおよびミーティングサポートおよび／または会議ソフトウェアが含まれる。

【００３５】可聴周波は放送位置限定チャネルを提供することができる媒体である。可聴周波は関係者が監視し、追跡することができる。交換の関係者は、可聴周波メッセージ中に何が搬送されているかを知らない場合でも、そのような可聴周波メッセージを送っているべき合法グループ関係者を認識することができる。可聴周波は、関係者にフィードバックを提供するために多くのソフトウェアによってすでに使用されている音声に組み込むことができる。例えば、たいていの団体会議コールセッティングは新しい関係者がコールに入るときはいつでも短い「ジョイントーン」をならす。そのようなトーンは関係者のキー情報を含有するようにも変更することができる。すでに可聴周波および／または音声情報を搬送するように設計された指定されたチャネルが存在するので、位置限定チャネルとしての可聴周波を電話ネットワークを介して使用することができる。

【００３６】位置限定チャネル上でパブリックキー暗号法を使用することはそれらの交換が機密を必要とせず、したがって盗聴されにくいことを意味するので、可聴周波チャネルの放送特性を使用してグループ通信を事前認証することができる。グループ通信の各関係者は、すべての他の合法関係者によって聞かれる可聴周波チャネル上でその関係者の事前認証情報を放送する。事前認証情報は概してパブリックキーへのコミットメントを含むことになる。放送はまた、攻撃者によって聞かれることがあるが、人間によってであろうとデバイスによってであろうと合法関係者によって検出されることなくそれらの攻撃者が可聴周波チャネル上でそれら自体の事前認証情報を放送するようにしないかぎり、それによってプロトコルのセキュリティが危険にさらされることはない。位置限定チャネル上で能動的攻撃を開始するためにそのように攻撃者の情報を放送しようと試みる攻撃者は通常、「余分な」放送があるので、合法人間またはデバイス関係者によって検出されることになる。例えば、可聴周波の場合、予期しない位置からの放送があることになる。

【００３７】合法関係者は、図２に関して説明したものなど知られているかまたは後で開発されたグループキー交換プロトコルを続行し、各関係者は、位置限定チャネル上で関係者によってコミットされたパブリックキーに対応するプライベートキーのその関係者の保有を１つまたは複数の合法関係者に証明する。そのようにコミットされたパブリックキーの１つに対応するパブリックキーの保有を証明することができる関係者はグループ通信中の認証される関係者と考えられる。さらに、選択されたキー交換プロトコルによりグループ通信の関係者間でさらなる通信を暗号化しかつ／または認証するために使用することができるいくつかの追加のキーをすべての関係者が共用することにもなる。

【００３８】図７～図９はネットワーク媒体上で無線デバイスのグループ間で通信を認証するための例示的なセッティングを示す。図７に示すように、１つの関係者がグループマネージャ６１０として働く。事前認証情報を送るべき第１の関係者はグループマネージャ６１０になる。その他の場合、ランダムな関係者がグループマネージャ６１０として選択される。グループマネージャ６１０は、放送位置限定チャネル上で様々な合法関係者６１２、６１４および６１６に事前認証段階中にグループパブリックキーへのコミットメントまたはそれ自身のパブリックキーなどの事前認証情報を放送する。図７に示すように、他の当事者６２２、６２４および６２６が存在し、無線ネットワークへのアクセス権を有する。位置限定チャネル上で送信しようと試みると、合法関係者は通常位置限定チャネル上のすべての送信を検出することができ、そのような送信の数を予想される送信の数、すなわち合法関係者の数と比較することができるので、その試みは検出されることになる。

【００３９】図８に示すように、各関係者６１２、６１４および６１６はグループマネージャ６１０からの認証放送情報に応答して、位置限定チャネル上でその関係者自身のパブリックキーへのコミットメントをそれぞれ含有するその関係者自身の事前認証情報をそれぞれ放送する。これらの放送はグループマネージャ６１０と他の合

法関係者６１２、６１４および６１６の両方によって受信される。その関係者の事前認証情報を放送した後、各関係者６１２、６１４および６１６は、例えば、グループマネージャの事前認証情報の一部としてグループマネージャ６１０によって提供されるアドレスを使用して、グループマネージ６１０へのポイントツーポイント接続を行う。各関係者６１２、６１４および６１６はＳｏｃｋｅｔＬａｙｅｒ／Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＳＳＬ／ＴＬＳ）などのポイントツーポイントキー交換プロトコルでグループマネージャ６１０に関与する。そのプロトコルを使用して、グループマネージャ６１０は関係者６１２、６１４および６１６の各々に共用される１つまたは複数のグループ暗号キーのコピーを与える。これらのキーは、グループマネージャ６１０および他の関係者６１２、６１４および６１６を含むすべての関係者間でさらなる通信を暗号化し、認証するために使用される。

【００４０】当事者６２２、６２４および６２６はそれらの事前認証情報を位置限定チャネル上で放送しなかったので、グループマネージャ６１０はグループ通信中に合法関係者として当事者６２２、６２４および６２６を認識しない。したがって、当事者６２２、６２４および６２６はグループマネージャ６１０と主無線リンク上でポイントツーポイント接続をうまく生成することはできないことになる。この結果、当事者６２２、６２４および６２６はグループマネージャ６１０およびすべての他の当事者６１２、６１４および６１６を含む合法関係者間でグループ通信を復号することを可能にするであろう共用グループキーを受信しないことになる。

【００４１】図１０はネットワーク媒体上で無線デバイスのグループ間で通信を認証する方法の第１の例示的な実施形態を概説するフローチャートである。オペレーションはステップＳ４００から始まり、ステップＳ４１０に進み、そこでグループの関係者のためのグループマネージャが選択される。ステップＳ４２０で、グループマネージャは位置限定チャネル上でそれの事前認証情報をグループの関係者に放送する。一実施形態による事前認証情報はグループマネージャのパブリックキーのダイジェストとすることができる。ステップＳ４３０で、グループマネージャの事前認証情報を受信する各関係者はそれの事前認証情報をグループマネージャおよび他の関係者に送ることによってこたえる。グループマネージャを含む関係者間での事前認証情報の交換は、放送として、位置限定チャネル上で行われる。一実施形態によれば、関係者の事前認証情報はその関係者のパブリックキーのダイジェストである。

【００４２】ステップＳ４４０で、グループマネージャおよび関係者の各々は、例えば無線リンク上で知られているかまたは後で開発されたキー交換プロトコルを使用して、事前認証段階中に受信したパブリックキーのダイジェストに対応するパブリックキーを使用してポイントツーポイントキー交換を実行する。そのようなプロトコルはまたグループマネージャとグループの現在関係者との間でポイントツーポイント暗号化および認証チャネルをセットアップすることになる。ステップＳ４５０で、グループマネージャは共用セッションキーとして使用されるべきグループキーのコピーを無線リンク上で各関係者に分配することができる。ステップ４６０で、認証方法のオペレーションは終わり、グループマネージャを含むグループの関係者間で確実な通信を続行することが可能になる。

【００４３】中央管理グループでは、関係者の加入および離脱を管理することは比較的容易である。加入する関係者はグループマネージャ６１０とともに上記で論じた２当事者プロトコルの１つを使用してそれ自体を認証し、保障された無線リンク上でグループキーを受信することができる。関係者がグループを離脱するとき、グループマネージャ６１０は無線リンク上ですべての残っている関係者に新しいグループキーを分配することができる。これはグループマネージャ６１０がポイントツーポイントキー交換中に各個別の関係者とともに共用シークレットキーを確立しているので行うことができる。

【００４４】図１１はネットワーク媒体上で無線デバイスのグループ間で通信を認証する別の方法を概説するフローチャートである。図１１に概説する方法によればすべての関係者が等しくキー生成に関係することができ、したがって、すべての関係者が等しく信用することができる。

【００４５】オペレーションはステップＳ５００で始まり、ステップＳ５１０に進み、そこで各関係者は、放送位置限定チャネルを使用してグループの関係者に、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパブリック値へのコミットメントなど、それの事前認証情報を放送する。ステップＳ５２０で、選択されたグループキー交換プロトコルを続行し、そこで関係者は無線ネットワーク上でそれらの完全なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパブリック値を提示する。グループキー交換プロトコルは、すべての関係者がグループ共用シークレットキーの生成を分担することを可能にする、グループの関係者間の変更Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎキー交換とすることができる。

【００４６】標準の２当事者Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎキー交換と同様に、シークレットが確立される間、グループの関係者は他人である。したがって、拡張Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎに基づくこれらのプロトコルは、すべての関係者が共用パブリックキーインフラストラクチャに関係するか、または前に交換されたパブリックキーを有することを仮定する。

【００４７】位置限定チャネル上で交換された事前認証情報により関係者は互いに認証することができるので、この仮定はもはや不要である。放送位置限定チャネルを

15　　16

使用するとグループのすべての関係者はそれらのパブリックキーを公的にグループの１つまたは複数の関係者にコミットすることができる。ステップＳ５３０で、関係者は次いで無線リンク上で選択されたグループキー交換プロトコルを続行し、例えば、提示された完全なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパブリック値を使用してグループキーを得る。オペレーションは次いでステップＳ５４０に進み、そこで認証方法のオペレーションは終わり、確実な通信を続行することが可能になる。

【００４８】セッションが始まった後で加入した関係者は、その関係者が加入する際に位置限定チャネル上でその関係者のキーコミットメントをグループの関係者の残りに放送することができる。ランダムに選択される現在関係者は応答して、相互認証を行うことができる。選択されたグループキー交換プロトコルは、これらの新しい関係者の共用グループキーを更新するか、または離脱する関係者のキーを無効にする詳細を扱うために使用される。

【図面の簡単な説明】

【図１】　本発明による通信認証システムを示す図である。

【図２】　本発明による無線デバイスを示す図である。

【図３】　本発明による通信を認証するための方法のフローチャートである。

【図４】　本発明による通信を認証するための方法のフローチャートである。

【図５】　本発明による通信を認証するための方法のフローチャートである。

【図６】　本発明による通信を認証するための方法のフローチャートである。

【図７】　本発明によるデバイスのグループの通信認証システムを示す図である。

【図８】　本発明によるデバイスのグループの通信認証システムを示す図である。

【図９】　本発明によるデバイスのグループの通信認証システムを示す図である。

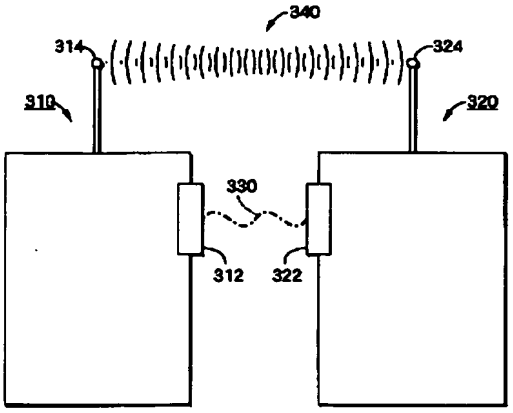
【図１０】　本発明による通信を認証するための方法のフローチャートである。

【図１１】　本発明による通信を認証するための方法の別のフローチャートである。

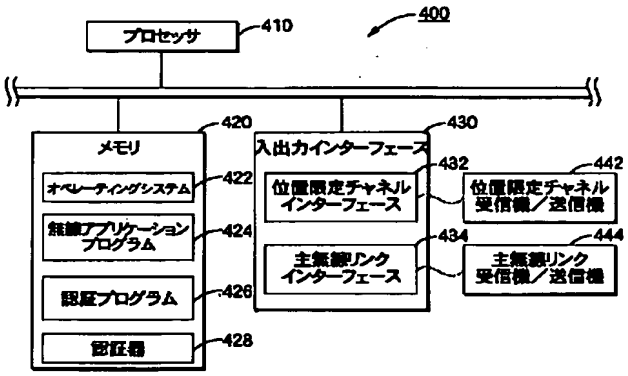
【符号の説明】

３００　無線システム、３１０　第１の無線デバイス、３１２　位置限定チャネル受信機／送信機、３１４　主無線リンク受信機／送信機、３２０　第２の無線デバイス、３２２　位置限定チャネル受信機／送信機、３２４　主無線リンク受信機／送信機、３３０　位置限定チャネル、４００　無線デバイス、４１０プロセッサ、４２０　メモリ、４２２　オペレーティングシステム、４２４　無線アプリケーション、４２６　認証アプリケーション、４２８　認証器、４３０入出力インターフェース、４３２　位置限定チャネルインターフェース、４３４　主無線リンクインターフェース、４４２　位置限定チャネル受信機／送信機、４４４　主無線リンク受信機／送信機。

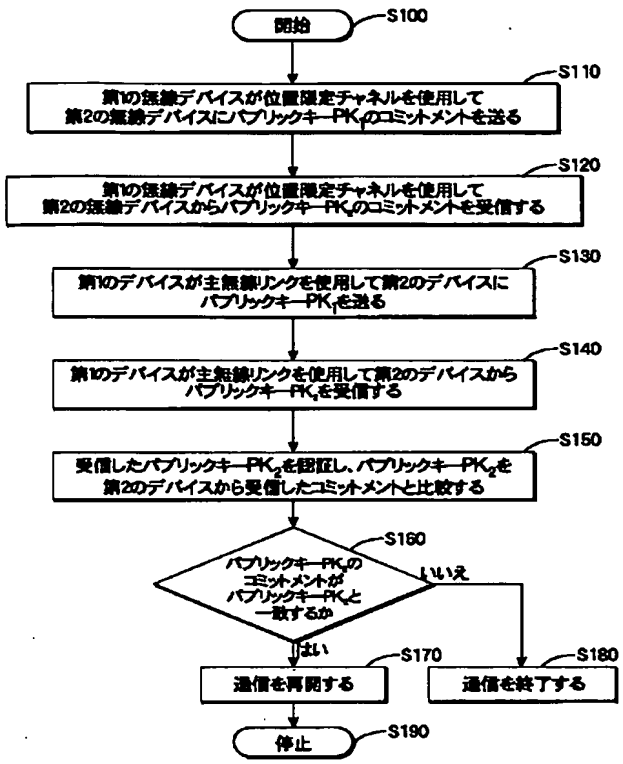
【図１】



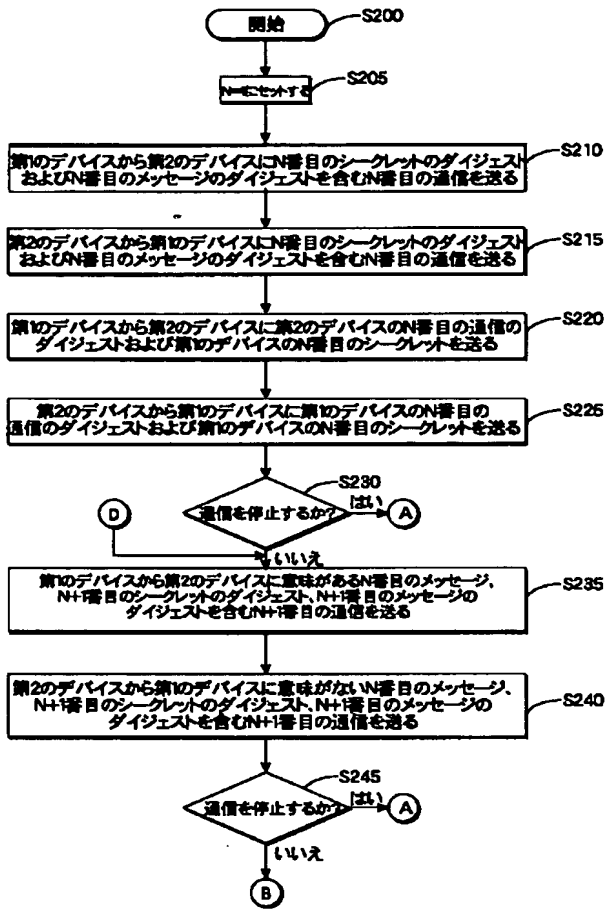
【図２】



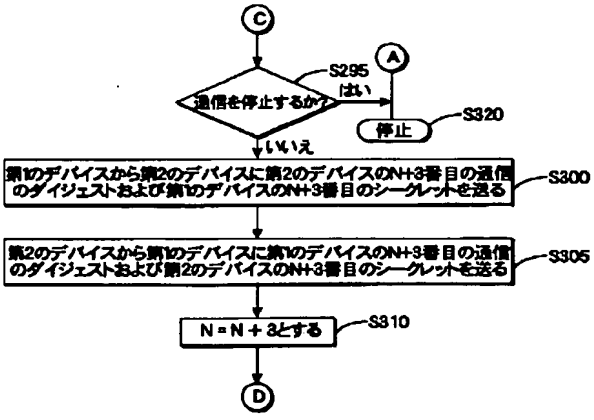
【図３】


開始
S100
第1の無線デバイスが位置限定チャネルを使用して第2の無線デバイスにパブリックキーPK1のコミットメントを送る
S110
第1の無線デバイスが位置限定チャネルを使用して第2の無線デバイスからパブリックキーPK2のコミットメントを受信する
S120
第1のデバイスが主無線リンクを使用して第2のデバイスにパブリックキーPK1を送る
S130
第1のデバイスが主無線リンクを使用して第2のデバイスからパブリックキーPK2を受信する
S140
受信したパブリックキーPK2を認証し、パブリックキーPK2を第2のデバイスから受信したコミットメントと比較する
S150
パブリックキーPK2のコミットメントがパブリックキーPK2と一致するか
S160
いいえ
はい
通信を再開する
S170
通信を終了する
S180
停止
S190

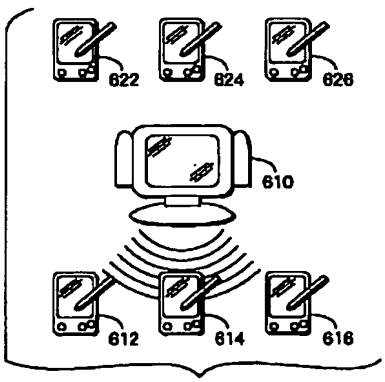
【図４】


開始
S200
Nをセットする
S205
第1のデバイスから第2のデバイスにN番目のシークレットのダイジェストおよびN番目のメッセージのダイジェストを含むN番目の通信を送る
S210
第2のデバイスから第1のデバイスにN番目のシークレットのダイジェストおよびN番目のメッセージのダイジェストを含むN番目の通信を送る
S215
第1のデバイスから第2のデバイスに第2のデバイスのN番目の通信のダイジェストおよび第1のデバイスのN番目のシークレットを送る
S220
第2のデバイスから第1のデバイスに第1のデバイスのN番目の通信のダイジェストおよび第1のデバイスのN番目のシークレットを送る
S225
通信を停止するか?
S230
はい
いいえ
D
A
第1のデバイスから第2のデバイスに意味があるN番目のメッセージ、N+1番目のシークレットのダイジェスト、N+1番目のメッセージのダイジェストを含むN+1番目の通信を送る
S235
第2のデバイスから第1のデバイスに意味がないN番目のメッセージ、N+1番目のシークレットのダイジェスト、N+1番目のメッセージのダイジェストを含むN+1番目の通信を送る
S240
通信を停止するか?
S245
はい
いいえ
A
B

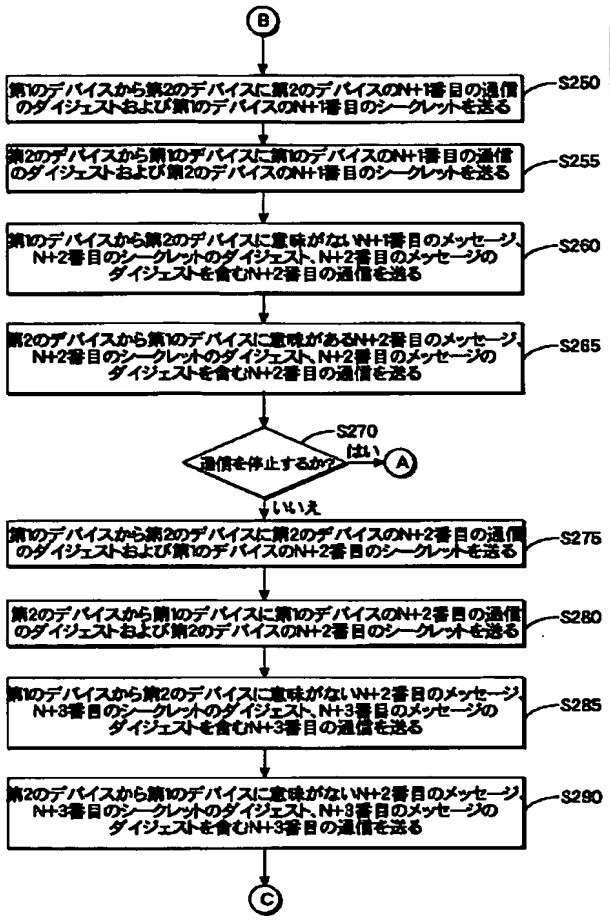
【図６】


C
通信を停止するか?
S295
はい
A
停止
S320
いいえ
第1のデバイスから第2のデバイスに第2のデバイスのN+3番目の通信のダイジェストおよび第1のデバイスのN+3番目のシークレットを送る
S300
第2のデバイスから第1のデバイスに第1のデバイスのN+3番目の通信のダイジェストおよび第2のデバイスのN+3番目のシークレットを送る
S305
N=N+3とする
S310
D

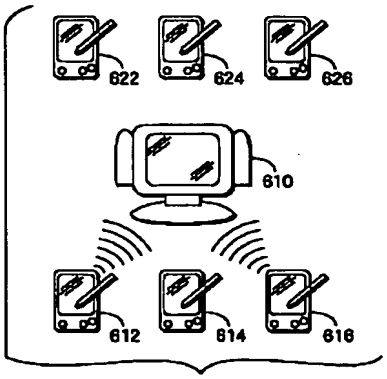
【図７】


622
624
626
610
612
614
616

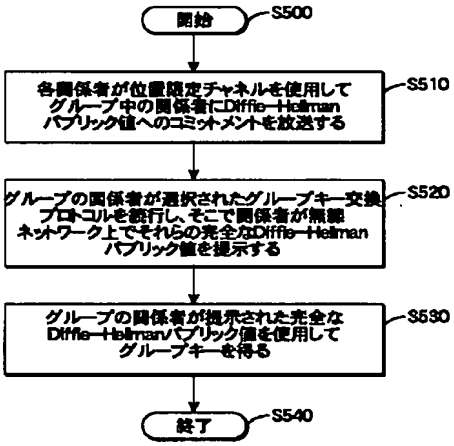
【図５】



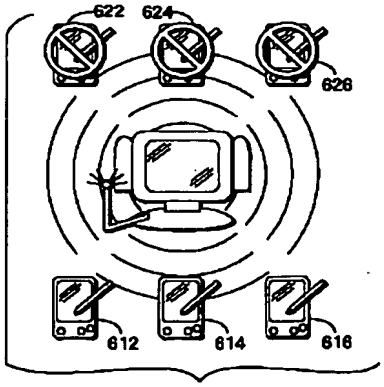
【図８】



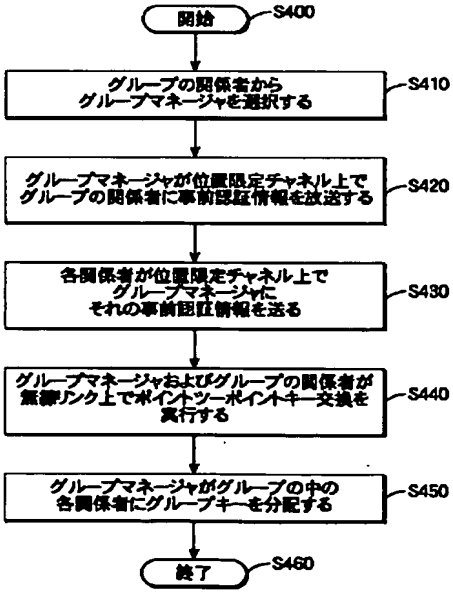
【図１１】



【図９】



【図１０】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
H04Q 7/38		H04L 9/00	601C

(72)発明者 クリスチーナ ブイ ロペス
アメリカ合衆国 カリフォルニア サンフランシスコ ゴンザレス ドライブ 750 #12エイチ
(72)発明者 ダイアナ ケイ シュメタース
アメリカ合衆国 カリフォルニア バーリンゲイム ラグーナ アベニュー 952
(72)発明者 ポール ジョセフ スチュワート
アメリカ合衆国 カリフォルニア サニーベイル ルイス ドライブ 864
(72)発明者 ハオ チー ウォン
アメリカ合衆国 カリフォルニア サンカルロス セダー ストリート 368

Fターム(参考) 5B085 AE04
5J104 AA01 AA07 AA16 EA04 EA19 EA21 EA24 JA21 KA02 KA05 KA06 NA02 NA12 NA24 PA01 PA07
5K033 AA08 CB01 CC01 DA02 DA17 DB14 DB16 EA03
5K067 AA30 DD17 DD23 EE02 EE25 GG01 GG11 HH22 HH23 HH24